CLAIMS

What is claimed is:

1. A method comprising:

receiving notification of a distributed denial of service attack;

establishing security authentication from an upstream router from which attack traffic, transmitted by one or more attack host computers, is received; and

once security authentication is established, transmitting one or more filters to the upstream router such that attack traffic is dropped by the upstream router, thereby terminating the distributed denial of service attack.

2. The method of claim 1, wherein detecting the attack traffic further comprises:

monitoring network traffic received by an Internet host; and

when a distributed denial of service attack is detected, notifying the Internet host of the distributed denial of service attack.

3. The method of claim 1, wherein establishing security authentication further comprises:

transmitting a security authentication request to the upstream router including authentication information, the authorization information including a destination address of the attack traffic; and

receiving authorization for establishment of security authentication from the upstream router.

4. The method of claim 1, wherein the transmitting the one or more filters further comprises:

identifying attack traffic characteristics of the attack traffic received by an Internet host;

generating one or more filters based on the identified attack traffic characteristics, such that the one or more filters direct the upstream router to drop network traffic matching the attack traffic characteristics;

digitally signing the one or more filters using a digital certificate of the Internet host; and

transmitting the one or more digitally signed filters to the upstream router.

5. A method comprising:

establishing security authentication of an Internet host under a distributed denial of service (DDoS) attack;

receiving one or more filters from the Internet host;

when security authentication is established, verifying that the one or more filters select only network traffic directed to the Internet host; and

once verified, installing the one or more filters such that network traffic matching the one or more filters is prevented from reaching the Internet host.

6. The method of claim 5, wherein establishing security authentication further comprises:

receiving a request for security authentication including authentication information from the Internet host;

selecting the authentication information from the security authentication request; and

authenticating an identity of the Internet host based on the selected authentication information.

7. The method of claim 5, wherein the receiving the one or more filters further comprises:

authenticating a source of the one or more filters received as the Internet host;

once authenticated, verifying that a router administrator has set a DDoS squelch time to live value for received filters;

once verified, generating a filter expiration time for each filter based on the time to live value, such that the filters are uninstalled once the expiration time expires;

verifying that an action component of each of the filters is drop; and

otherwise, disregarding the one or more filters received from the Internet host.

8. The method of claim 5, wherein verifying the one or more filters further comprises:

selecting a destination address component for each of the one or more filters received from the Internet host;

comparing the selected destination address components against an address of the Internet host;

verifying that the selected destination addresses matches the Internet host address; and

otherwise, disregarding the one or more filters received from the Internet host.

9. The method of claim 5, wherein installing the one or more filters further comprises:

selecting network traffic matching one or more of the filters received from the Internet host; and

dropping the selected network traffic such that attack traffic received from one or more attack host computers by the Internet host is eliminated in order to terminate the distributed denial of service attack.

10. The method of claim 5, further comprising:

determining, by an upstream router receiving the one or more filters from the Internet host, one or more ports from which the attack traffic matching the one or more filters is being received based on a routing table;

selecting a port from the one or more determined ports;

determining an upstream router connected to the selected port based on a routing table;

securely forwarding the one or more filters received from the Internet host to the detected upstream router as a routing protocol update; and

repeating the selecting, determining and utilizing for each of the one or more determined ports.

11. A method comprising:

receiving a routing protocol update from a downstream router;

selecting one or more filters from the routing protocol update received from the downstream router;

establishing security authentication of the downstream router;

once authentication is established, verifying that the one or more filters select only network traffic directed to the downstream router; and

once verified, installing the one or more filters such that attack traffic matching the one or more filters is prevented from reaching the downstream router.

12. The method of claim 11, wherein establishing security authentication of the downstream router further comprises:

selecting authentication information from the routing protocol update received from the downstream router;

once selected, authenticating an identity of the downstream router based on the authentication information;

authenticating a source of the one or more filters as the downstream router;

once authenticated, verifying that a router administrator has set a DDoS squelch time to live value for received filters;

once verified, generating a filter expiration time for each filter based on the time to live value, such that the filters are uninstalled once the expiration time expires;

verifying that an action component of each of the filters is drop; and

otherwise, disregarding the one or more filters received from the downstream router.

13. The method of claim 11, wherein verifying the one or more filters further comprises:

selecting a destination address component for each of the one or more filters;

comparing the selected destination address component against an address of the downstream router;

verifying that the selected destination address matches the downstream router address; and

otherwise, disregarding the one or more filters received from the downstream router.

14. The method of claim 11, further comprises:

determining, by an upstream router receiving the one or more filters from the downstream router, one or more ports from which attack traffic matching the one or more received filters is being received;

selecting a port from the one or more determined ports;

determining an upstream router coupled to the selected port based on a routing table;

securely forwarding the one or more received filters to the determined upstream router as a routing protocol update; and

repeating the selecting, determining, and forwarding for each of the one or more determined ports.

15. A computer readable storage medium including program instruction that directed a computer to function in a specific manner when executed by a processor, the program instructions comprising:

receiving notification of a distributed denial of service attack;

establishing security authentication from an upstream router from which attack traffic, transmitted by one or more attack host computers, is received; and

once security authentication is established, transmitting one or more filters to the upstream router such that attack traffic is dropped by the upstream router, thereby terminating the distributed denial of service attack.

16. The computer readable storage medium of claim 15, wherein the instruction of detecting the attack traffic further comprises:

monitoring network traffic received by an Internet host; and

when a distributed denial of service attack is detected, notifying the Internet host of the distributed denial of service attack.

17. The computer readable storage medium of claim 15, wherein establishing security authentication further comprises:

transmitting a security authentication request to the upstream router including authentication information, the authorization information including a destination address of the attack traffic; and

receiving authorization for establishment of security authentication from the upstream router.

18. The apparatus of claim 15, wherein transmitting the one or more filters further comprises:

identifying attack traffic characteristics of the attack traffic received by an Internet host;

generating one or more filters based on the identified attack traffic characteristics, such that the one or more filters direct the upstream router to drop network traffic matching the attack traffic characteristics;

digitally signing the one or more filters using a digital certificate of the Internet host; and

transmitting the one or more digitally signed filters to the upstream router.

19. A computer readable storage medium including program instruction that directed a computer to function in a specific manner when executed by a processor, the program instructions comprising:

establishing a security authentication of a downstream device;

once security authentication is established, verifying that one or more filters from the downstream device select only network traffic directed to the downstream device; and

once verified, installing the one or more filters such that network traffic matching the one or more filters is prevented from reaching the downstream device.

20. The apparatus of claim 19, wherein establishing security authentication further comprises:

receiving a routing protocol update from the downstream device;

selecting authentication information from the received routing protocol update;

authenticating an identity of the downstream device based on the selected authentication information;

once authenticated, selecting the one or more filters from the received routing protocol; and

authenticating integrity of the one or more filters based on a digital signature of the filters.

21. The apparatus of claim 19, wherein verifying the one or more filters further comprises:

authenticating a source of the one or more filters received as the downstream device;

once authenticated, verifying that a router administrator has set a DDoS squelch time to live value for received filters;

once verified, generating a filter expiration time for each filter based on the time to live, such that the filters are uninstalled once the expiration time expires;

verifying that an action component of each of the filters is drop; and

otherwise, disregarding the one or more filters received from the Internet host.

22. The apparatus of claim 19, wherein verifying the one or more filters further comprises:

selecting a destination address component for each of the one or more filters received from the downstream device;

comparing the destination address components against an address of the downstream device;

verifying that the selected destination addresses matches the downstream device address; and

otherwise, disregarding the one or more filters received from the downstream device.

23. The computer readable storage medium of claim 19, wherein establishing security authentication further comprises:

receiving a request for security authentication including authentication information from the downstream device;

selecting the authentication information from the security authentication request; and

authenticating an identity of the downstream device based on the selected authentication information.

24. The apparatus of claim 19, wherein installing the one or more filters further comprises:

selecting network traffic matching one or more of the filters received from the downstream device; and

dropping the selected network traffic such that attack traffic received from one or more attack host computers by the downstream device is eliminated in order to terminate a distributed denial of service attack.

25. The apparatus of claim 19, further comprising:

determining, by an upstream router receiving the one or more filters from the downstream router, one or more ports from which attack traffic matching the one or more received filters is being received;

selecting a port from the one or more determined ports;

determining an upstream router coupled to the selected port based on a routing table;

securely forwarding the one or more received filters to the determined upstream router as a routing protocol update; and

repeating the selecting, determining, and forwarding for each of the one or more determined parts.

26. An apparatus, comprising:

a processor having circuitry to execute instructions;

a control plane interface coupled to the processor, the control plane interface to packet processing filers, and to authenticate a source of the packet processing filters; ad

a storage device coupled to the processor, having sequences of instructions stored therein, which when executed by the processor cause the processor to:

establish a security authentication of a downstream device.

once security authentication is established, verify that one or more filters from the downstream device select only network traffic directed to the downstream device and

once verified, install the one or more filters such that network traffic matching the one or more filters is prevented from reaching the downstream device..

27. The apparatus of claim 26, wherein the instruction to establish security authentication further causes the processor to:

receive a routing protocol update from the downstream device;

select authentication information the received from routing protocol update;

authenticate an identity of the downstream device based on the selected authentication information;

once authenticated, select the one or more filters from the received routing protocol; and

authenticate integrity of the one or more filters based on a digital signature of the filters.

28. The apparatus of claim 26, wherein the instruction to receive the one or more filters further causes the processor to:

authenticate a source of the one or more filters received as the downstream device;

once authenticated, verify that a router administrator has set a DDoS squelch time to live value for received filters;

once verified, generate a filter expiration time for each filter based on the time to live, such that the filters are uninstalled once the expiration time expires;

verify that an action component of each of the filters is drop; and

otherwise, disregard the one or more filters received from the Internet host.

29. The apparatus of claim 26, wherein the instruction to verify the one or more filters further causes the processor to:

select a destination address component for each of the one or more filters received from the downstream device,

compare the destination address components against an address of the downstream device,

verify the selected destination addresses matches the Internet host address, and

otherwise, disregard the one or more filters received from the downstream device

30. The apparatus of claim 26, wherein instruction to install the one or more filters further causes the processor to:

select network traffic matching one or more of the filters received from the downstream device, and

drop the selected network traffic such that attack traffic received from one or more host attack computers by the downstream device is eliminated in order to terminate a distributed denial of service attack.

31. The apparatus of claim 26, wherein the processor is further caused to:

determine, by a router receiving the one or more filters from the downstream device, one or more ports from which the attack traffic matching the one or more filters is being received based on a routing table,

determine one or more upstream routers connected to the determined ports,

establish a secure connection with each of the one or more upstream routers, and

forward the one or more filters received from the downstream device to the one or more upstream routers.

32. The apparatus of claim 26, wherein the instruction to establish security authentication further causes the processor to:

receiving a request for security authentication including authentication information from the downstream device;

decrypting the received authentication information;

selecting the authentication information from the security authentication request; and

authenticating an identity of the downstream device based on the selected authentication information.

33. A system comprising:

an Internet host;

a wide area network; and

a router coupled between the Internet host and the wide area network, the router having:

a processor having circuitry to execute instructions;

a control plane interface coupled to the processor, the control plane interface to receive packet processing filers, and to authenticate a source of the packet processing filters; and

a storage device coupled to the processor, having sequences of instructions stored therein, which when executed by the processor cause the processor to:

establish security authentication of an Internet host under a distributed denial of service (DDoS) attack;

receive one or more filters from the Internet host;

when security authentication is established, verify that the one or more filters select only network traffic directed to the Internet host; and

once verified, install the one or more filters such that network traffic matching the one or more filters is prevented from reaching the Internet host.

34. The system of claim 33,

wherein the Internet host receives notification of a distributed denial of service attack, establishes security authentication from an upstream router from which the attack traffic, transmitted by one or more attack host computers, is received, and transmits one or more filters to the upstream router such that attack traffic is dropped by the upstream router, thereby terminating the distributed denial of service attack.

35. The system of claim 33, wherein the processor is further caused to:

determine, by a router receiving the one or more filters from a downstream device, one or more ports from which the attack traffic matching the one or more filters is being received based on a routing table,

determine one or more upstream routers connected to the determined ports, and

securely forward the one or more filters received from the downstream device to the one or more upstream routers as a routing protocol update.